REMARKS

The Applicants request reconsideration of the rejection.

Claims 1-13 remain pending, with claims 5-13 under consideration pursuant to withdrawal of claims 1-4.

The Examiner notes, on page 2 of the Office Action, that the amended specification refers to "An Introduction to the Theory of Cryptography", which has not been filed with an Information Disclosure Statement. Applicants are filing herewith an Information Disclosure Statement including this reference.

The specification has also been amended to clarify the source of the mode of disclosure.

The Examiner further objected to the specification and rejected claims 5-10 under 35 U.S.C. §112, first and second paragraphs, citing a lack of clarity and/or support in the expression "in order of its bit sequence." Claim 5 has been amended to clarify that step (b) is that, after transferring one operation unit in the bit pattern of data A in a memory in order of bit sequence of said data A to a first register R1, one operation unit in the bit pattern of data B is transferred in order of bit sequence of said data B to a second register R2. Step (c) has been amended similarly, as have similar steps in independent claim 6.

By these amendments, it is believed clear that one operation unit of data A or data B in a memory is transferred to a register in order or its own bit sequence. The Applicants refer the Examiner, for example, to Fig. 22 and its related description. In

other words, after an operation result of A[j] and B[j] is stored in C[j], "j" is incremented in order.

Claims 11-13 were rejected under 35 U.S.C. §102(e) as being anticipated by Kocher et al., U.S. Patent No. 6,327,661 (Kocher). The Applicants traverse as follows.

Claim 11 is limited by a step (c) of transferring one operation unit in a bit pattern of data B in the memory corresponding to one operation unit of data A to a second register R2. Step (a) requires any one unprocessed operation unit in a bit pattern of data A to be randomly selected. Thus, one operation unit of data A is associated beforehand with one operation unit of data B, and the method randomly selects an unprocessed operation unit of data A to execute an arithmetic operation for the selected operation unit and the corresponding operation unit of data B, according to step (d) ("executing the predetermined arithmetic operation for the contents of said first register R1 (storing the selected operation unit of data A) and the contents of said second register R2 (storing the transferred operation unit in the bit pattern of data B)"). By this feature of the invention, because a randomly selected operation unit of data A can be supplied for the arithmetic operation independently of the other operation units of data A, it is far more difficult to estimate the whole of data A or data B than in the case of processing data A and data B in order of their bit sequences. On the other hand, Kocher discloses in col. 12, lines 45-60 to perform a blinding operation in which, for each loop iteration, a random number generator produces a random blinding bit, a temporary buffer is initialized with the XOR of the

random bit and an input data bit, the input data bit being selected according to a previously constructed table, and an output buffer is initialized with the blinding bit, where the blinding bit is the result of using the input permutation table to operate on the index to the temporary buffer. The second part of the blinding process re-randomizes the bit order of permutation table. Finally, input bits are loaded in the order specified by the table, permuted according to the externally specified permutation table, and XORed onto the destination table. Thus, the two consecutive XOR operations gives the result of the original data bit, which in effect is merely the relocation of the input data as the output data.

According to the invention, both data A and data B are significant data, and data A has an associated relationship with data B, whereas Kocher's input data has no such association with the blinding data. Even supposing that the input data is significant data, the blinding data is temporarily generated. Neither data A nor data B are randomly arranged bits, however, unlike Kocher's blinding data, and thus both data A and data B are significant and thus different by comparison with Kocher.

Because Kocher teaches no more than the random selection of an input data bit and relocation thereof, the Applicants respectfully submit that the present invention is neither anticipated nor rendered obvious by Kocher, whether taken individually or in combination with any other reference of record.

The Applicants note with thanks the allowability of claims 5-10.

In view of the foregoing amendments and remarks, Applicants contend that the above-identified application is now in condition for allowance. Accordingly, reconsideration and reexamination are respectfully requested.

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Mattingly, Stanger, Malur & Brundidge, P.C., Deposit Account No. 50-1417 (referencing attorney docket no. NIT-294).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

Daniel J. Stanger
Registration No. 32,846

DJS/sdb
(703) 684-1120